Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A computer program product for a client computing system including a processor includes:

code that directs the processor to request a challenge from an authentication server;

code that directs the processor to receive the challenge from the authentication server via a first secure communications channel, wherein the challenge ~~comprising~~ comprises an identity code;

code that directs the processor to receive user authentication data from a user;

code that directs the processor to determine a private key and a digital certificate in response to the user authentication data;

code that directs the processor to form a digital signature in response to the identity code from the authentication server and the private key;

code that directs the processor to communicate the digital signature to the authentication server,

code that directs the processor to communicate the digital certificate to the authentication server, the digital certificate comprising a public key in an encrypted form; and

code that directs the processor to communicate network user authentication data and the identity code to the authentication server via a security server,

wherein the authentication server activates the identity code when the digital signature is verified, and

wherein the codes reside on a tangible media.

2. (Original) The computer program product of claim 1 wherein the identity code remains inactivate when the authentication server does not verify the digital signature.

3. (Currently amended) The computer program product of claim 1 wherein the security server comprises a server selected from ~~the class~~ a group of servers consisting of: firewall server, VPN gateway server.

4. (Original) The computer program product of claim 1 wherein code that directs the processor to determine the private key and the digital certificate in response to the user authentication data comprises code that directs the processor to determine a private key associated with the user when the user authentication data is correct.

5. (Original) The computer program product of claim 4 wherein code that directs the processor to determine the private key and the digital certificate in response to the user authentication data further comprises code that directs the processor to determine a private key not associated with the user when the user authentication data is incorrect.

6. (Original) The computer program product of claim 1 further comprising code that directs the processor to receive network user authentication data from the user.

7. (Original) The computer program product of claim 1 wherein code that directs the processor to receive user authentication data from a user comprises code that directs the processor to receive user authentication data and the network authentication data from the user.

8. (Currently amended) A client computing system for communicating with a private server includes:

a tangible memory configured to store a key wallet, the key wallet including a private key associated with the user and a digital certificate associated with a user, the private key and digital certificate stored in an encrypted form;

a processor coupled to the tangible memory, the processor configured to receive a challenge from an authentication server via a first secure communications channel, the challenge comprising an identity code, configured to receive user authentication data from the user, configured to determine a retrieved private key and a retrieved digital certificate from the key wallet in response to the user authentication data from the user; configured to form a digital signature in response to the identity code received from the authentication server and the retrieved private key, configured to communicate the digital signature to the authentication server, configured to communicate the digital certificate to the authentication server, and configured to communicate network user authentication data and the identity code to the authentication server via a security server,

wherein the authentication server activates the identity code when the digital signature is verified, and

wherein the security server allows the client computing system to communicate with the private server when the identity code is activated.

9. (Original) The client computing system of claim 8 wherein the retrieved private key and the private key associated with the user are identical.

10. (Original) The client computing system of claim 8

wherein the retrieved private key and the private key associated with the user are different, and

wherein when the retrieved private key and the private key associated with the user are different the identity code remains inactive.

12. (Currently amended) The client computing system of claim 8 wherein the security server comprises a server selected from ~~the class~~ a group of servers consisting of:

firewall server, VPN gateway server, electronic mail server, web server, database server, database system, application server.

13. (Original) The client computing system of claim 8 wherein the tangible memory can be removed from the client computer.

14. (Original) The client computing system of claim 8 wherein the processor is also configured to receive the network user authentication data from the user.

15. (Currently amended) A client system for communicating with a remote server includes:

a tangible memory configured to store key wallet program, the key wallet program configured to store a private key associated with the user and a digital certificate associated with a user in protected forms;

means for receiving a challenge from a verification server via a first secure communications channel, the challenge comprising at least a network password that is inactive;

means for receiving at least a PIN from the user;

means coupled to the tangible memory for determining a returned private key and a returned digital certificate from the key wallet in response to at least the PIN from the user;

means for forming a digital signature in response to the network password received from the verification server and to the private key;

means for communicating the digital certificate and the digital signature to the authentication server; and

means for communicating at least the network password to a security server,

wherein the network password is activated when the digital signature and digital certificate authenticate the user; and

wherein the security server allows the client system to communicate with the remote server when the network password is activated.

16. (Original) The client system of claim 15 wherein the returned private key and the private key associated with the user are the same.

17. (Currently amended) The client system of claim 16

wherein the means for determining a returned private key comprises means for determining the returned private key in response to the PIN from the user, and a pre-determined PIN, wherein when the PIN from the user and the pre-determined PIN are different, the returned private key is different from ~~and~~ the private key associated with the user ~~are different~~, wherein when the PIN from the user and the pre-determined PIN are the same, the returned private key is the private key associated with the user;

wherein when the returned private key and the private key associated with the user are different the digital signature and the digital certificate do not authenticate the user.

18. (Original) The client system of claim 15 further comprising means for receiving at least a network password associated with the user from the user,

wherein the means for communicating the digital certificate and the digital signature to the authentication server also comprise means for communicating the network password associated with the user to the authentication server.

19. (Original) The client system of claim 15 wherein the means for communicating the digital certificate and the digital signature to the authentication server also comprise means for communicating a network password associated with the user to the authentication server;

the client system further comprising means for determining the network password associated with the user in response to at least the PIN from the user.

20. (Currently amended) The client computing system of claim 15 wherein the client computing system is selected from ~~the class~~ a group of devices consisting of: desktop computer, portable computer, PDA, wireless device.

21. (New) The client computing system of claim 8

wherein the identity code is determined in the authentication server, and

wherein the identity code is not stored on the client computing system before receiving the challenge from the authentication server.